IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	**10/803,945**	Confirmation No. 7176
Applicant	:	K. SHIMOOKA et al.	
Filed	:	March 19, 2004	
Title	:	DATA PROTECTING APPARATUS AND METHOD, AND COMPUTER SYSTEM	
TC/AU	:	2132	
Examiner	:	Barron Jr., G.	
Docket No.	:	TSM-37	
Customer No.:		24956	

MAIL STOP PETITIONS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESUBMISSION
OF
PETITION TO MAKE SPECIAL
(ACCELERATED EXAMINATION UNDER 37 CFR §1.102(d))

Sir:

On February 8, 2005, the Applicants filed a Petition to Make Special for Accelerated Examination in accordance with 37 CFR §1.102(d) and MPEP § 708.02(VIII). However, to-date, no decision on the Petition has been issued. A check of the application file on private pair shows that the Preliminary Amendment, filed on the same date as the Petition, was properly entered into the case, but the Petition itself was not entered. Accordingly, Applicants are resubmitting the Petition. Further, Applicants have modified their discussion of the references in this

Resubmission to better distinguish the claims of the application from the cited references.

PETITION TO MAKE SPECIAL

Applicants petition the Commissioner to make the above-identified application special in accordance with 37 CFR §1.102(d). In support of this Petition, pursuant to MPEP § 708.02(VIII), Applicants state the following.

(A) REQUIRED FEE

This Petition when originally filed was accompanied by the fee set forth in 37 CFR § 1.117(h). The Commissioner is hereby authorized to charge any additional payment due, or to credit any overpayment, to Deposit Account No. 50-1417.

(B) ALL CLAIMS ARE DIRECTED TO A SINGLE INVENTION

Following the Preliminary Amendment filed on February 8, 2005, claims 1-7, 9-17, and 19-20 are pending in the application. All the pending claims of the application are directed to a single invention. If the Office determines that all claims in the application are not directed to a single invention, Applicant will make election without traverse as a prerequisite to the grant of special status in conformity with established telephone restriction practice.

As set forth in independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20, the claimed invention is generally directed to an intrusion detection and data protection system

and method for a computer system. Under claim 1, the invention is a data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between said computer and said storage volume, wherein said data protection apparatus comprises: an event detection unit for detecting an event occurrence; and a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit detects an event.

Additionally, under independent claim 4, the invention is a data protection method for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume and a storage control unit for controlling communication between said computer and said storage volume, wherein said data protection method comprises steps of: detecting an event occurrence; and disconnecting a path to stop communication between said computer and said storage volume, when said event is detected.

Further, under independent claim 5, the invention is a program for making an information processing apparatus perform data protection of a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between

said computer and said storage volume, wherein said program makes said information processing apparatus perform processes of: detecting an event occurrence; and disconnecting a path to stop communication between said computer and said storage volume, after said event is detected.

Also, under independent claim 6, the invention is a computer system comprising a storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a storage control unit for controlling communication between said computer and said storage volume, and a data protection apparatus for protecting data in said storage volume, wherein: said data protection apparatus comprises: an event detection unit for detecting an event occurrence; and a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit detects an event.

Furthermore, under independent claim 7, the invention is a data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said data protection apparatus comprises: an event detection unit for detecting an event occurrence; and a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event; said

computer system further comprising a computer for reading and writing data from and to said storage volume; an illegal intrusion detection unit for detecting an illegal intrusion into said computer; wherein said event detection unit receives a detection of the illegal intrusion from said illegal intrusion detection unit; and when said event detection unit receives the detection of the illegal intrusion, said replication stopping unit instructs said storage control unit to stop data transfer from said storage volume to said replicated volume.

In addition, under independent claim 10, the invention is a data protection method for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a replicated volume assigned for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said data protection method comprises steps of: detecting an intrusion into said computer; and instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said intrusion is detected.

Also, under independent claim 11, the invention is a program for making an information processing apparatus perform data protection of a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a replicated volume assigned for storing data duplicated from said

storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said program makes said information processing apparatus perform processes of: detecting that an intrusion into the computer has occurred; and instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said intrusion is detected.

Additionally, under independent claim 14, the invention is a computer system comprising a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, a storage control unit for controlling data transfer from said storage volume to said replicated volume, and a data protection apparatus for protecting data in said storage volume, wherein: said data protection apparatus comprises: an event detection unit for detecting an event occurrence; and a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event; wherein said computer system further comprises an alteration detection unit that reads given data in said plurality of replicated volumes to detect respective differences between the given data; and the event detected by said event detection unit is a detection result of the differences between the given data, with said detection result being received from said alteration detection unit.

Finally, under independent claim 20, the invention is a computer system comprising: a storage apparatus comprising a storage volume assigned for storing

data, a replicated volume assigned for storing data duplicated from said storage volume, a host computer for reading and writing data from and to said storage volume, a storage control unit for controlling communication between said host computer and said storage volume, and a data protection apparatus for protecting data in said storage volume, wherein: said host computer detects an illegal intrusion and sends a notification of the detected illegal intrusion to said data protection apparatus; said data protection apparatus receives said notification and gives said storage control unit an instruction to disconnect a path to stop communication between said computer and said storage volume; and said storage control unit, receiving said instruction, rejects access from outside to the storage volume of said storage apparatus.

(C) PRE-EXAMINATION SEARCH

A pre-examination search has been conducted, directed to the invention as claimed. The pre-examination search was conducted in the following US Manual of Classification areas:

Class	Subclass
365	222
709	224
711	162, 163
713	200, 201

Furthermore, a keyword search was conducted on the USPTO's EAST database. Additionally, a literature search was also conducted for relevant non-patent documents using the Association for Computing Machinery online databases.

In addition, a search for foreign patent documents was conducted on the ESPACENET databases.

(D) REFERENCES DEEMED MOST-CLOSELY RELATED TO THE SUBJECT MATTER ENCOMPASSED BY THE CLAIMS

Based upon a review of the documents located by the search and the documents already of record in the application, the references deemed to be most-closely related to the subject matter encompassed by the claims are listed below. These documents were made of record in the present application by the Information Disclosure Statements filed on January 13, 2005, and June 4, 2004.

Patent/App. No.	**Inventor(s)**
US 5918008	Togawa, Yoshifusa et al.
US 20010007120	Makita, Satoshi
US 20040010732	Oka, Nobuyuki
US 20040025044	Day, Christopher W.
US 20040078636	Suzaki, Kuniyasu
US 20040117401	Miyata, Kenichi et al.
US 20040143761	Mendonca, John et al.

Publication

6.3.3. "Intrusion Detection Systems", Introduction to Network Management for Beginners, in Foundation for Multimedia Communications, Network Management Section, (online), May 15, 2002.

Because all of the above-listed documents are already of record in the present application, in accordance with MPEP § 708.02(VIII)(D), additional copies of these documents have not been submitted with this Petition.

(E) DETAILED DISCUSSION OF THE REFERENCES

Following a brief discussion of the invention, the references deemed most-closely related are discussed below in Section (E)2, pointing out, with the particularity required by 37 CFR 1.111 (b) and (c), how the claimed subject matter is patentable over the teachings of these documents.

1. Discussion of the Invention

As set forth in claims 1 and 6, a first feature of the invention includes a path disconnection unit for instructing the storage control unit to stop communication between the computer and the storage volume, when the event detection unit detects an event.

Additionally, as set forth in claims 4 and 5, a second feature of the invention is a method or program that includes disconnecting a path to stop communication between the computer and the storage volume, when an event is detected.

Additionally, as recited in claim 7, a third feature of the invention includes that when an event detection unit receives the detection of an illegal intrusion, a replication stopping unit instructs the storage control unit to stop data transfer from the storage volume to a replicated volume.

Similarly, as set forth in claims 10 and 11, a fourth feature of the invention is a method or program that includes instructing the storage control unit to stop data transfer from the storage volume to a replicated volume, when an intrusion is detected.

Also, as set forth in claim 14, a fifth feature of the invention includes a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event.

Further, as set forth in claim 20, a sixth feature of the invention is a data protection apparatus that receives a notification of detected illegal intrusion and gives a storage control unit an instruction to disconnect a path to stop communication between a computer and a storage volume, wherein the storage control unit, receiving the instruction, rejects access from outside to the storage volume of the storage apparatus.

Accordingly, from the foregoing, it may be seen that the present invention provides for stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6 and 20. The invention also provides for stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as recited in claims 7, 10, 11 and 14. It is submitted that the cited references, whether taken individually, or in combination, fail to teach or suggest the invention as claimed in independent claims 1, 4, 5, 6, 7, 10, 11, 14, and 20.

2. Discussion of the References Deemed to be Most-Closely Related

The patent to Togawa et al., US 5918008, shows a storage device having a function for coping with a computer virus. The device includes a virus checker that

detects whether a file stored on a disk is infected with a virus with reference to an infection management table. When a judging means has judged that a file is infected with a virus, a prohibiting means prohibits use of the file. (See, e.g., Abstract and column 2, lines 23-36.) Thus, Togawa et al. do not teach the present invention, including stopping communication between a computer and a storage volume, or stopping data transfer from a storage volume to a replicated volume, upon the detection of an event or intrusion. More particularly, Togawa et al. do not teach that communication is stopped between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Rather, Togawa et al. prohibit use of a file. Further Togawa et al. do not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14. Togawa et al. provide no disclosure regarding replicated volumes.

The published US patent application to Makita, US 20010007120, shows a storage device connected to a host computer. The storage device includes a virus check unit that makes it unnecessary for the host computer to perform a virus check, thus reducing a processing load imposed on the host computer. The virus check unit performs a virus check at a time of recording a file on, or reading out a file from a recording medium, or based on a frequency of accesses from the one of the host computers to the recording medium. When a virus is discovered, storing the information on the recording medium is halted, and the host computer is notified that

the virus is discovered. (See, e.g., Abstract and paragraphs 62-63 and 172-176.) However, Makita does not teach the present invention, wherein communication is stopped between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Rather, Makita stops storing information on a recording medium, and provides no teaching regarding storage volumes or communication therewith. Further, Makita provides no teaching for stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14. Makita provides no disclosure regarding replicated volumes.

The published US patent application to Oka, US 20040010732, is assigned to the same assignee as the present invention (for purposes of 35 USC 103 (c)), and shows a backup method and storage control device in which performing the backup includes: having the storage control device allocate a specified number of generations of the backup volume in the storage device for the copy volume; instructing the storage device to split a pair of volumes; executing a virus check on the copy volume of the pair; copying the contents of the checked copy volume to the backup volume as a most recent generation backup for the copy volume if no virus is detected by the virus check; updating the generations in the backup volume for generations prior to the most recent generation; and instructing the storage device to re-link the split pair. If a virus is detected as a result of a virus check based on virus definition update scheduling information, information looked-up or updated from the

generation/backup/restore target management module is used to perform a restore while the system is in a degraded operating state in which an attribute indicating unavailability is applied to the primary volume and the copy volume. Alternatively, the system can be stopped. (See, e.g., Abstract, and paragraphs 8, 21, 39-46 and 57.) However, Oka does not teach the present invention, since changing a volume attribute to indicate unavailability does not necessarily stop communication between a computer and a storage volume, or stop replication. Thus, Oka does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, Oka does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14. Rather, Oka teaches checking a copy volume for viruses before replicating data to a backup volume.

The published US patent application to Day, US 20040025044, shows an intrusion detection system that includes an anomaly detector and a classifier that can classify detected anomalous correlations based upon at least one configurable correlation metric. Where anomalous behavior has been classified as an event, individual clusters associated with the anomalous behavior can be further examined to determine whether an unauthorized network intrusion has occurred. (See, e.g., Abstract, and paragraphs 35-37.) However, Day does not teach stopping communication between a computer and a storage volume, or stopping replication,

when an event or intrusion is detected. More particularly, Day does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, Day does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14.

The published US patent application to Suzaki, US 20040078636, shows a system with an input and output means for a computer system storage. The system includes a computer equipped with a first storage, a second storage that with respect to access speed operates at a higher speed than the first storage, and a processor. A virtual computer operating on the computer is included, and is equipped with a configuration that, when writing to the first storage, writes via a disk cache of a predetermined capacity. A data transfer path from the disk cache to a hard disk of the first storage is provided with a switch to control the flow of data, thereby controlling whether or not there are hard-disk rewrites. (See, e.g., Abstract, and paragraphs 16-18, 31-35.) Thus, Suzaki does not disconnect upon the occurrence of an event, and does not teach the present invention, including stopping communication between a computer and a storage volume, or replication, when an event or intrusion is detected. More particularly, Suzaki does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, Suzaki

does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14.

The published US patent application to Miyata, US 20040117401, is assigned to the same assignee as the present invention (for purposes of 35 USC 103 (c)), and shows an information processing system that includes a storage device system 16 that has an interface 161 for connection with a scan server 15 and a storage device 162 that contains a virus database. Scan server 15 includes an interface 151 for connection with network 12; a CPU 152; a memory 153 containing an OS 1531 and a virus scanner 1532; a network 154 in the scan server; and an interface 155 for connection with storage device system 16. CPU 152 executes virus scanner 1532, which compares a suspected file with associated patterns contained in virus database 1621. If a file is infected, the host CPU notifies a client that the file cannot be opened. (See, e.g., Abstract and paragraphs 17-19 and 21.) Thus, Miyata does not stop communication between a computer and a storage volume, or replication, when an event or intrusion is detected. More particularly, Miyata does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, Miyata does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14.

The published US patent application to Mendonca, US 20040143761, is directed to an intrusion detection system in a provisionable network. The system includes: evaluating the system security of the provisionable network; and applying a system lockdown in the provisionable network in accordance with the results of the evaluation. (See, e.g., Abstract and paragraphs 14-15.) However, Mendonca does not stop communication between a computer and a storage volume, or stop replication, when an event or intrusion is detected. More particularly, Mendonca does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, Mendonca does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14.

The publication "Intrusion Detection Systems" provides a general discussion of intrusion detection systems for detecting in real time attempts to intrude into a network. Responses to a detected intrusion taught by the publication include displaying an alert notice, starting an external application, storing and studying the generated event, session cutoff, changing firewall rules and denying packets in question, and restoring the original contents of system file or registry which have been changed. (See, e.g., last two pages of the publication.) Thus, the publication does not teach stopping communication between a computer and a storage volume, or stopping replication, when an event or intrusion is detected. More particularly, the

publication does not teach stopping communication between a computer and a storage volume when an event or intrusion is detected, as set forth in claims 1, 4, 5, 6, and 20. Additionally, the publication does not teach stopping data transfer from a storage volume to a replicated volume when an event or intrusion is detected, as set forth in claims 7, 10, 11 and 14.

(F) CONCLUSION

As demonstrated by the above discussion, the references fail to teach or suggest a path disconnection unit for instructing the storage control unit to stop communication between the computer and the storage volume, when the event detection unit detects an event, as set forth in claims 1 and 6.

The references also fail to teach or suggest a method or program that includes disconnecting a path to stop communication between the computer and the storage volume, when an event is detected, as set forth in claims 4 and 5.

The references also fail to teach or suggest that when an event detection unit receives the detection of an illegal intrusion, a replication stopping unit instructs the storage control unit to stop data transfer from the storage volume to a replicated volume, as recited in claim 7.

Similarly, the references also fail to teach or suggest a method or program that includes instructing the storage control unit to stop data transfer from the storage volume to a replicated volume, when an intrusion is detected, as set forth in claims 10 and 11.

The references also fail to teach or suggest a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event, as set forth in claim 14.

The references also fail to teach or suggest a data protection apparatus that receives a notification of detected illegal intrusion and gives a storage control unit an instruction to disconnect a path to stop communication between a computer and a storage volume, wherein the storage control unit, receiving the instruction, rejects access from outside to the storage volume of the storage apparatus, as set forth in claim 20.

Thus, it is submitted that all of these claims are patentable over the cited references taken individually, or in combination with each other. The remaining claims are dependent claims, claim additional features of the invention, and are patentable at least because they depend from allowable base claims. Accordingly, the requirements of 37 CFR §1.102(d) having been satisfied, the Applicants request that this Petition to Make Special be granted and that the application be examined according to prescribed procedures set forth in MPEP §708.02 (VIII).

The Applicants prepared this Petition in order to satisfy the requirements of 37 C.F.R. §1.102(d) and MPEP §708.02 (VIII). The pre-examination search required by these sections was "directed to the invention as claimed in the application for which special status is requested." MPEP §708.02 (VIII). The search performed in support of this Petition is believed to be in full compliance with the requirements of MPEP

§708.02 (VIII); however, Applicants make no representation that the search covered every conceivable search area that might contain relevant prior art. It is always possible that prior art of greater relevance to the claims may exist. The Applicants urge the Examiner to conduct his or her own complete search of the prior art, and to thoroughly examine this application in view of the prior art cited above and any other prior art that may be located by the Examiner's independent search.

Further, while the Applicants have identified and discussed certain portions of each cited reference in order to satisfy the requirement for a "detailed discussion of the references, which discussion points out, with the particularly required by 37 C.F.R. §1.111(b) and (c), how the claimed subject matter is patentable over the references" (MPEP §708.02(VIII)), the Examiner should not limit review of these documents to the identified portions, but rather is urged to review and consider the entirety of each reference.

(G) FEE PAYMENT (37 C.F.R. 1.17(h))

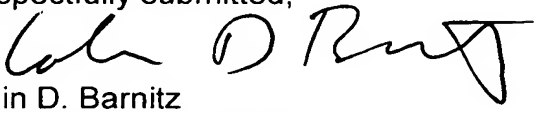
The fee required by 37 C.F.R. § 1.17(h) is to be paid by:

[ ] the Credit Card Payment Form (attached) for $130.00.

[ ] charging Account 50-1417 the sum of $130.00.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417. A duplicate of this petition is attached.

Respectfully submitted,



Colin D. Barnitz
Registration No. 35,061

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
703-684-1120
Date: July 18, 2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22314
(703) 684-1120

TSM-37

Appl. No.	:	**10/803,945**
Applicant	:	K. SHIMOOKA et al.
Filed	:	March 19, 2004
Title	:	DATA PROTECTING APPARATUS AND METHOD, AND COMPUTER SYSTEM
TC/AU	:	2818
Examiner	:	TBA
Docket No.	:	TSM-37
Customer No.:		24956

Confirmation No. 7176

Papers Filed Herewith:

Transmittal Letter;
PRELIMINARY AMENDMENT;
PETITION TO MAKE SPECIAL; and
Credit Card Payment Form in the amount of $130.00
in payment of petition to make special fee.

Receipt is hereby acknowledged of the papers filed, as identified in connection with the above-identified patent application.

COMMISSIONER FOR PATENTS